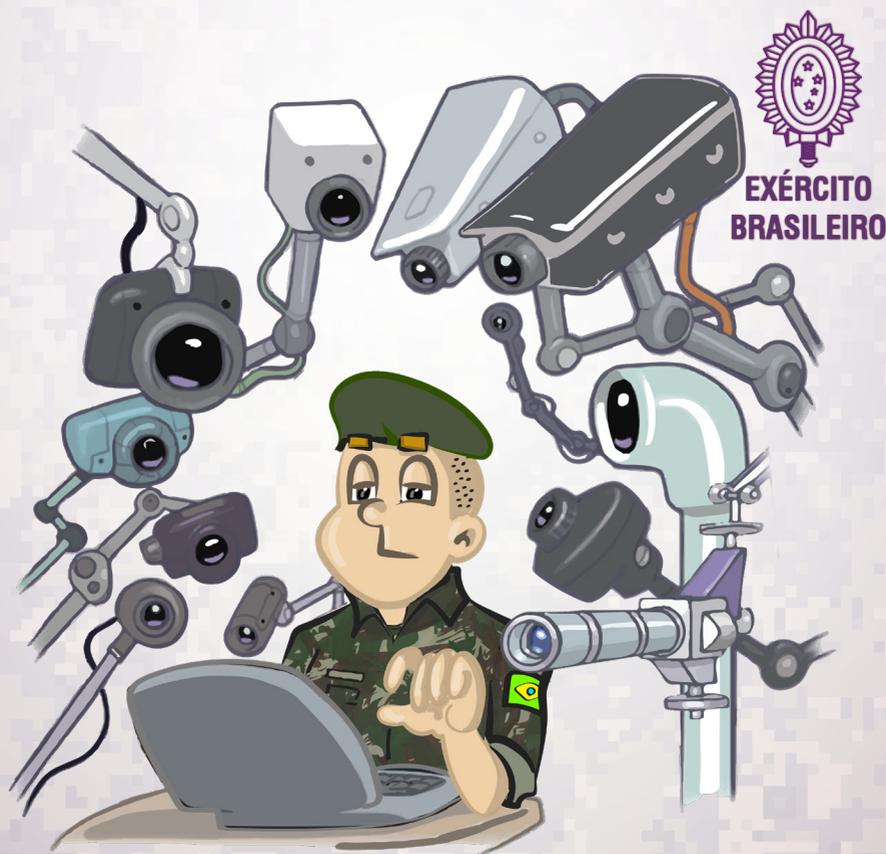
Campanha de Conscientização Cibernética

PRIVACIDADE

VALORIZE SUA PRIVACIDADE

Não é porque você não tem nada a esconder que precisa abrir mão de sua **privacidade**. A exposição excessiva e a coleta abusiva de dados podem dar a outros a capacidade de influenciar e limitar suas escolhas, além de facilitar a ação de pessoas mal-intencionadas.

Veja aqui dicas de como cuidar de sua privacidade e segurança na Internet.

PENSE BEM ANTES DE POSTAR ALGO

Depois que **algo** é enviado ou **postado** na Internet, **dificilmente** pode ser **apagado** ou ter seu acesso controlado. Alguém pode já ter copiado e passado adiante.

» Não compartilhe conteúdo do qual **possa se arrepender** depois

» Considere que você está em um **local público**:

- tudo o que você posta pode ser visto por alguém, tanto agora como no futuro

Lembre-se:
uma vez postado, sempre postado.

MANTENHA A INTIMIDADE OFFLINE

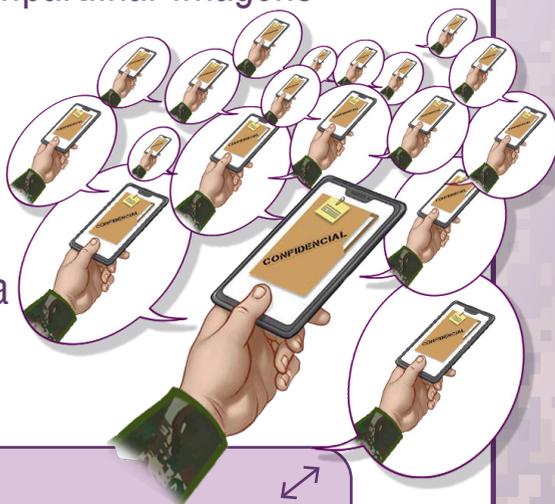
Fotos e vídeos íntimos podem ser usados para constranger e chantagear as pessoas que aparecem neles. É preciso tomar **cuidado** com imagens da **intimidade**.

» Evite compartilhar imagens ou se deixar filmar ou fotografar em **situações íntimas**

» **Apague** fotos e vídeos antes de levar dispositivos para a assistência técnica

» Oriente **crianças e jovens** sobre os riscos de exposição da intimidade

» Se realmente quiser compartilhar imagens íntimas:

- evite mostrar o rosto ou marcas que possam identificá-lo, como **cicatrizes e tatuagens**
- use **temporizador** para apagar as mensagens automaticamente

Lembre-se:
a Internet não guarda segredos.

RESPEITE E PROTEJA A PRIVACIDADE DAS CRIANÇAS

Você já parou para pensar o impacto que pode gerar ao **expor crianças** na Internet?
Que algo que você considera “bonitinho” pode causar **constrangimento** e ***bullying***?
Que imagens sem roupa, como no banho, podem vazar e acabar em redes de **pedofilia**?

- » Evite fazer e compartilhar imagens de crianças **com pouca roupa**
  - proteja a galeria de fotos do celular com **senha ou biometria**
  - se precisar enviar foto por mensagem para o médico, use temporizador para apagar
- » Evite fazer postagens que exponham a rotina de seus filhos
- » Respeite os limites de idade das redes sociais e de jogos

AJUSTE AS CONFIGURAÇÕES DE SEGURANÇA E PRIVACIDADE

Sistemas, *sites* e aplicativos costumam **oferecer opções** para que você controle como suas informações serão usadas e compartilhadas. Mas é comum que as configurações padrão sejam permissivas e precisem ser adequadas a suas necessidades.

» Avalie e ajuste as configurações de segurança e privacidade
  - procure o **equilíbrio** entre exposição, segurança e privacidade

LIMITE AS PERMISSÕES DE ACESSO DOS APLICATIVOS

Para funcionar, muitos aplicativos **solicitam permissões**, como acesso à câmera, microfone, geolocalização, redes e contatos. Alguns acessos são essenciais, mas outros podem ser abusivos e comprometer sua privacidade e segurança.

» Ao instalar e usar um aplicativo, autorize apenas acessos **compatíveis** com sua finalidade

REDUZA A COLETA DE INFORMAÇÕES DE NAVEGAÇÃO

Os *sites* que você acessa podem **coletar informações** de seu navegador para identificá-lo e rastreá-lo, saber por onde navega, suas buscas e escolhas. Desta forma, podem traçar seu perfil e oferecer conteúdos personalizados para **influenciá-lo**, ou até mesmo limitar suas opções.

» Limite a coleta de dados por *cookies*
  - configure o navegador para **não aceitar *cookies* de terceiros**
  - nos sites que permitem escolha, autorize somente ***cookies* essenciais**

» Use o modo de navegação anônima, quando possível

FORNEÇA APENAS INFORMAÇÕES NECESSÁRIAS

Ao preencher **formulários e cadastros**, muitas vezes são coletadas informações além das necessárias. Em muitos casos, elas são usadas para traçar seu perfil e fazer anúncios direcionados; em outros, são vendidas para terceiros.

» Questione-se sobre a necessidade de fornecer todos os dados e da instituição retê-los
  - não forneça, se entender que a solicitação é **abusiva ou desnecessária**

SEJA SELETIVO AO ACEITAR SEGUIDORES NAS REDES SOCIAIS

Quanto maior sua rede, maior o acesso a seus dados, postagens e lista de contatos. Isso aumenta o risco de **abuso dessas informações** e de perda de privacidade, tanto sua como de seus contatos. Aceitar qualquer contato também facilita a ação de pessoas mal-intencionadas.

» Configure sua conta como **privada**, quando possível

» Verifique a identidade da pessoa antes de aceitá-la em sua rede

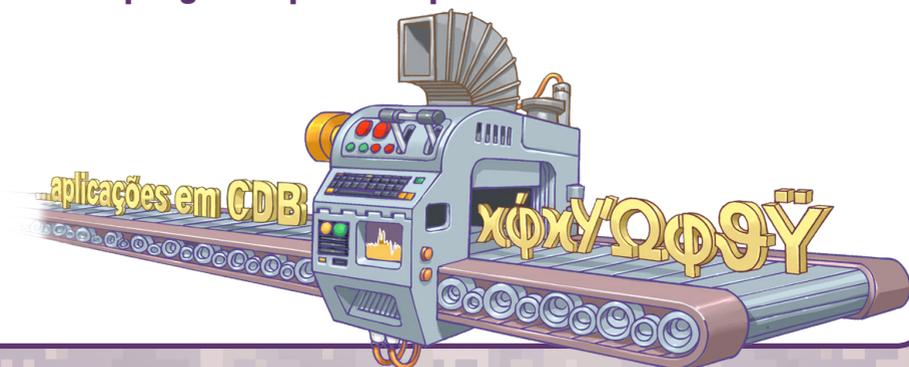
- **bloqueie** contas falsas

USE CRIPTOGRAFIA PARA PROTEGER OS DADOS

A criptografia protege os dados, de modo que sejam lidos e entendidos somente por quem tem autorização. É importante que seja usada tanto ao transmitir informações pela rede, como para armazená-las.

» Use **conexões seguras**, como *https* para acesso a sites, e VPN para acesso remoto
  • além de **cifrar** os dados, garante que você está conectando no **destino correto**

» Ative a criptografia em celulares, *tablets*, disco do computador e mídias removíveis, como disco externo

» Prefira usar aplicativos de mensagem com **criptografia ponta a ponta**

PROTEJA SUAS CONTAS E SENHAS

Se suas contas forem **invadidas**, sua identidade pode ser furtada e usada para praticar fraudes em seu nome, causando prejuízos a você e a seus contatos. Você também pode ser espionado e se tornar **vítima de extorsão**, com ameaças de vazamento de informações ou fotos.

» Use **verificação em duas etapas**, sempre que possível
» Use **senhas fortes**, difíceis de adivinhar
» **Não repita** senhas
  - uma senha vazada pode levar à invasão de outras contas

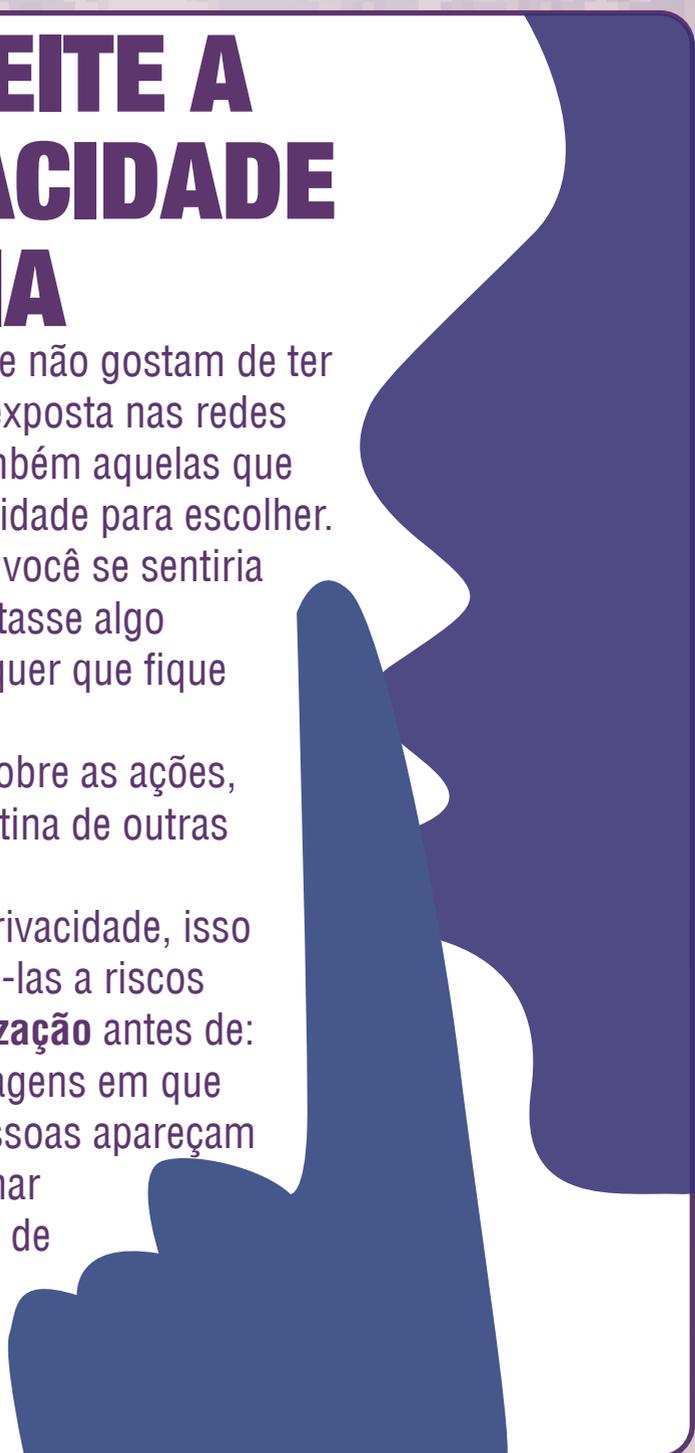
EVITE COMPARTILHAR SENHAS OU DISPOSITIVOS

Quem tiver acesso a suas senhas e dispositivos pode **acessar suas informações** e, sem querer ou de propósito, instalar códigos maliciosos. Se algum *spyware* for instalado, pode espioná-lo, rastrear sua localização, ver suas postagens, tirar e copiar fotos suas e depois chantageá-lo.

» **Desconfie** se pedirem sua senha como prova de amor ou amizade
  - quem o ama de verdade respeita sua privacidade

» Se precisar compartilhar um dispositivo, **limite o acesso**:
  - crie perfis separados, sempre que possível
  - trave o aplicativo específico na tela
  - use **controle parental** se for usado por crianças

Há pessoas que não gostam de ter a privacidade exposta nas redes sociais. Há também aquelas que ainda não têm idade para escolher. Imagine como você se sentiria se alguém postasse algo que você não quer que fique público.

- Evite falar sobre as ações, hábitos e rotina de outras pessoas
  - além da privacidade, isso pode expô-las a riscos
- Peça **autorização** antes de:
  - postar imagens em que outras pessoas apareçam
  - compartilhar postagens de outras pessoas

UTILIZE MECANISMOS DE PROTEÇÃO NO COMPUTADOR

Certos tipos de *malware* espionam o usuário, coletando informações para depois aplicar golpes, por vezes, com extorsão. Antivírus e *firewall* pessoal ajudam a proteger os dispositivos contra *malware* e ataques vindos da Internet.

» Instale um antivírus (*antimalware*) e mantenha-o **atualizado**
» Assegure-se de ter um *firewall* pessoal instalado e ativo

INFORME-SE SOBRE AS POLÍTICAS DE PRIVACIDADE

Antes de fornecer seus dados em sites e aplicativos, é importante saber como eles serão tratados. Isso ajuda a identificar práticas abusivas de coleta e compartilhamento de dados que possam comprometer sua privacidade e segurança.

» Entenda:
- quais dados são coletados
- para quais finalidades serão utilizados
- com quem podem ser compartilhados

» **Não aceite** e não use o serviço se não concordar com os termos

» Informe-se sobre a **Lei Geral de Proteção de Dados (LGPD)** e conheça seus direitos

APAGUE OS DADOS DE DISPOSITIVOS QUE NÃO USA MAIS

Vai trocar seu celular ou *tablet*, descartar ou repassar para outra pessoa? Lembre-se de que ele está cheio de **informações pessoais** e, se não forem apagadas, podem ser indevidamente acessadas.

» Desconecte sua conta ID de sistema

» Restaure as configurações originais (“de fábrica”)

» Retire cartões de memória e chip SIM

» Remova o dispositivo da lista de dispositivos confiáveis em suas contas

FIQUE ATENTO À SEGURANÇA DE DISPOSITIVOS CONECTADOS

Dispositivos conectados podem conter falhas de segurança em diferentes elementos (dispositivo, aplicativo, nuvem), gerando riscos como vazamentos de dados e invasão de privacidade.

» Antes da compra, **pesquise** o produto/fabricante por:
  • reputação quanto à segurança e privacidade
  • disponibilidade de correções de segurança
  • modo de tratamento, armazenamento e transmissão de seus dados

» Evite deixar **assistentes virtuais em espera**, "ouvindo" o tempo todo
  • e cubra possíveis câmeras "indiscretas"

Dispositivos conectados, como relógios, assistentes virtuais, câmeras de vídeo e brinquedos, costumam enviar dados para a nuvem, incluindo dados sobre saúde, localização e gravações de voz e imagem.

REFLITA SE COMPENSA TROCAR SEUS DADOS POR DESCONTOS

Você já pensou por que tantas empresas pedem para você fazer cadastro e informar o CPF a cada compra? O “desconto” é a **contrapartida** para que você autorize a coleta e o uso de seus dados. Assim, elas passam a conhecê-lo melhor e podem selecionar o que ofertar ou mesmo deixar de ofertar.

» Antes de cair na tentação dos programas de desconto, analise:
  • para que seus dados serão usados e com quem serão compartilhados?
  • os valores dos descontos compensam sua exposição?
  • será que podem limitar suas opções no futuro?

» Reflita também sobre o potencial risco de **vazamentos de dados**
  • você pode acabar sendo vítima de golpes

SAIBA MAIS
Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais fascículos da Campanha de Conscientização Cibernética no site EB.MIL.BR

EXÉRCITO BRASILEIRO

Novos Desafios, Mesmos Valores

Produção: